BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) UK Patent Application (19) GB (11) 2 079 837 A

(21) Application No 8119650
(22) Date of filing
25 Jun 1981
(30) Priority data
(31) 168615
(32) 14 Jul 1980
(33) United States of America (US)
(43) Application published
27 Jan 1982
(51) INT CL³ E05B 47/00
(52) Domestic classification
E2A LV
F1B 2Z
(56) Documents cited
GB 2026081A
GB 2014237A
GB 2010375A
GB 1525003
GB 1229730
GB 1152831
GB 1114373
(58) Field of search
E2A
F1B
G4V
(71) Applicant
John Lee Royster
1985 South 12th East
Apartment 9
Salt Lake City
Utah 84105
United States of America
(72) Inventor
David A Soss
(74) Agents
Mathisen Macara & Co
Lyon House
Lyon Road
Harrow
Middlesex HA1 2ET

(54) Security locking system

(57) A security locking system for preventing the unauthorized operation of a vehicle or entry into a dwelling house or the like includes a transmitting unit and a receiving unit. The receiving unit is mounted and concealed inside the vehicle or dwelling house and the transmitting unit is a hand-held portable, self powered, device, which generates a magnetic field over a limited range that varies according to a uniquely coded sequence. When the transmitting unit is in close proximity to the receiving unit, the presence of the varying magnetic field will be sensed by the receiving unit, and if correctly coded it will allow power to flow from a power source to an enabling element of the device to be secured, e.g. the vehicle's ignition system or a solenoid valve located in the vehicle's fuel line.

GB 2079837 A

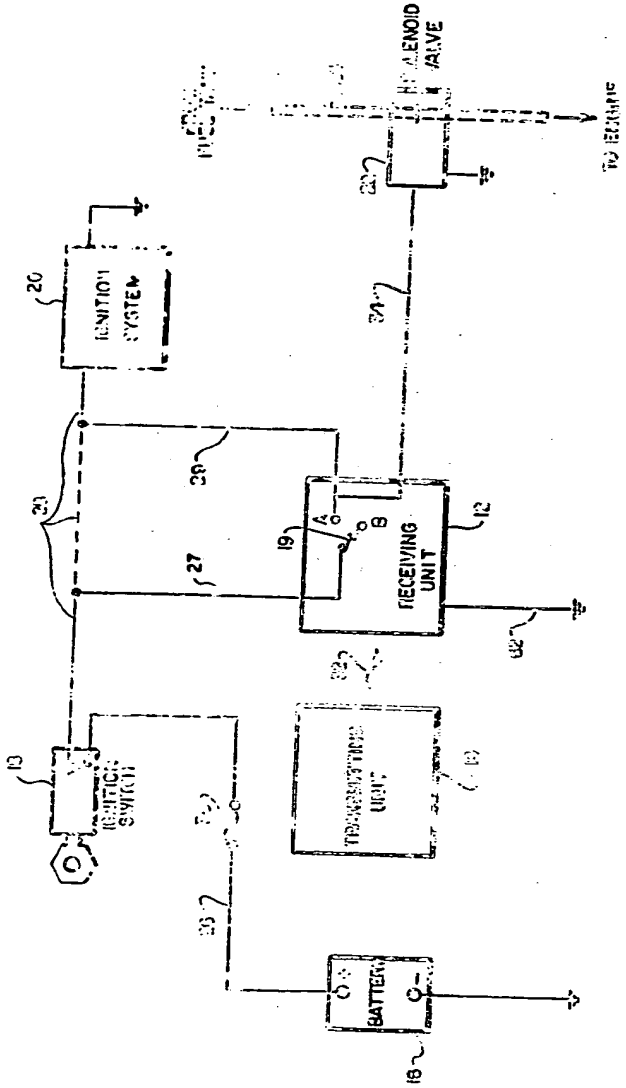
SOLENOID VALVE
TO ENGINE
IGNITION SYSTEM
20
24
26
23
27
19
A
B
RECEIVING UNIT
12
22
IGNITION SWITCH
13
TRANSMITTING UNIT
25
BATTERY
18

Fig. 1

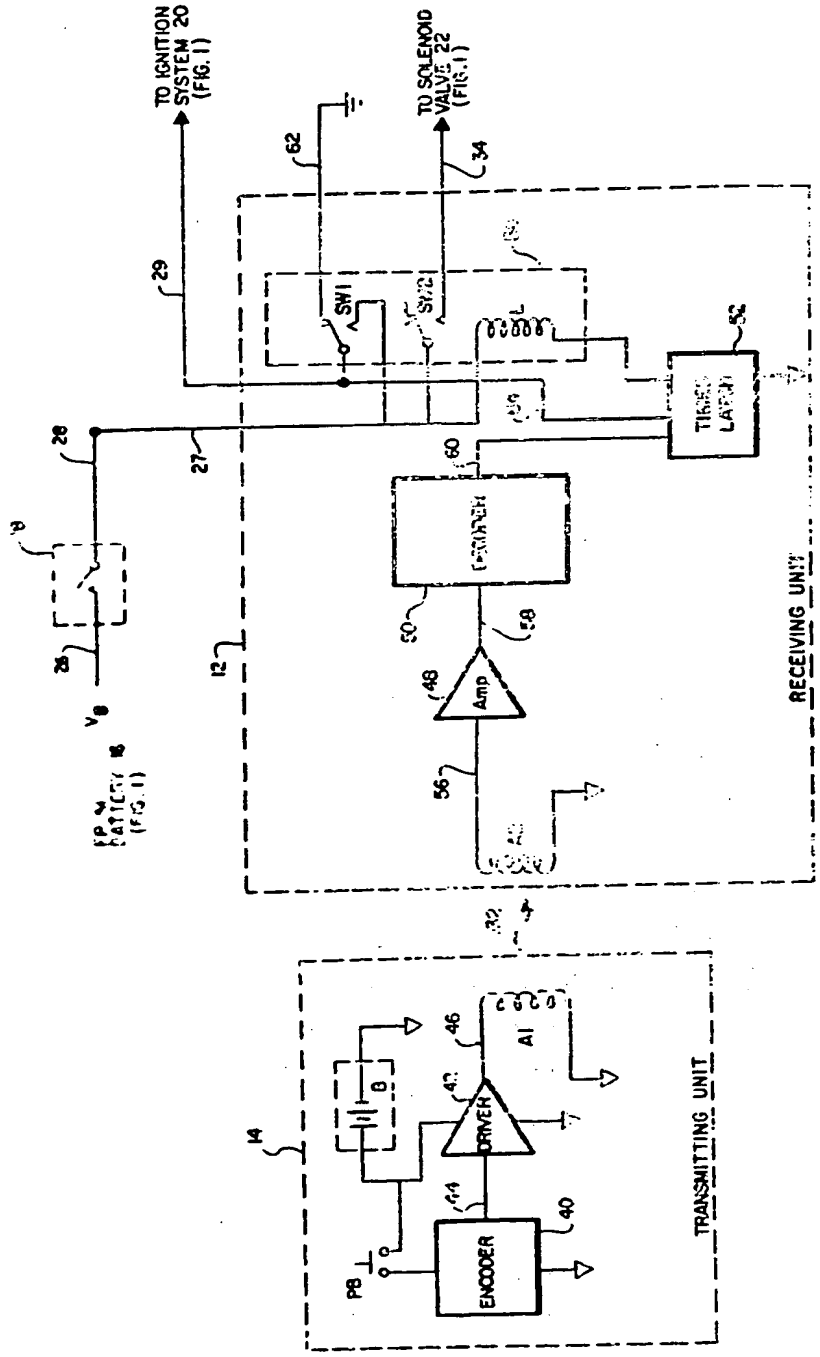

Fig. 2

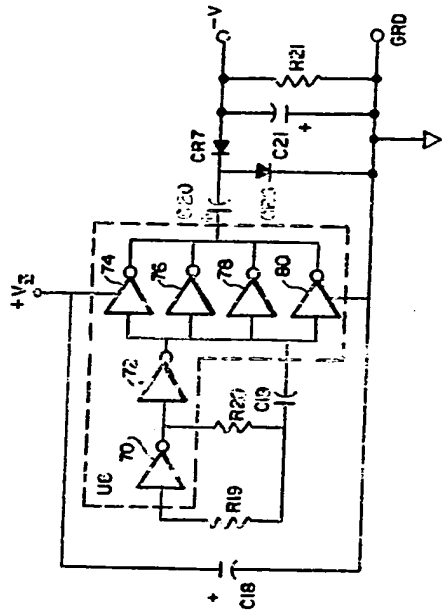
-V
GRD
R21
C21
CR7
C20
+V3
74
76
78
80
72
R20
C19
70
U6
R19
C18

Fig. 5

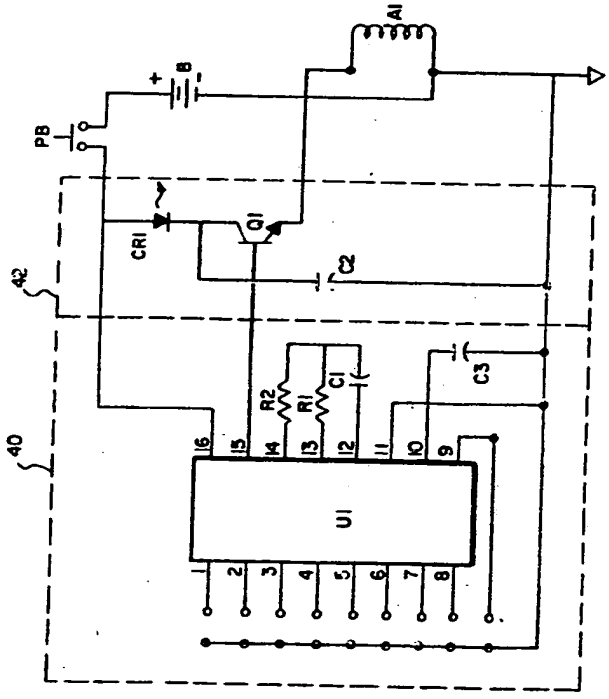
A1
B
PB
CR1
Q1
C2
42
R2
R1
C1
C3
40
16
15
14
13
12
11
10
9
U1
2
3
4
5
6
7
8

Fig. 3

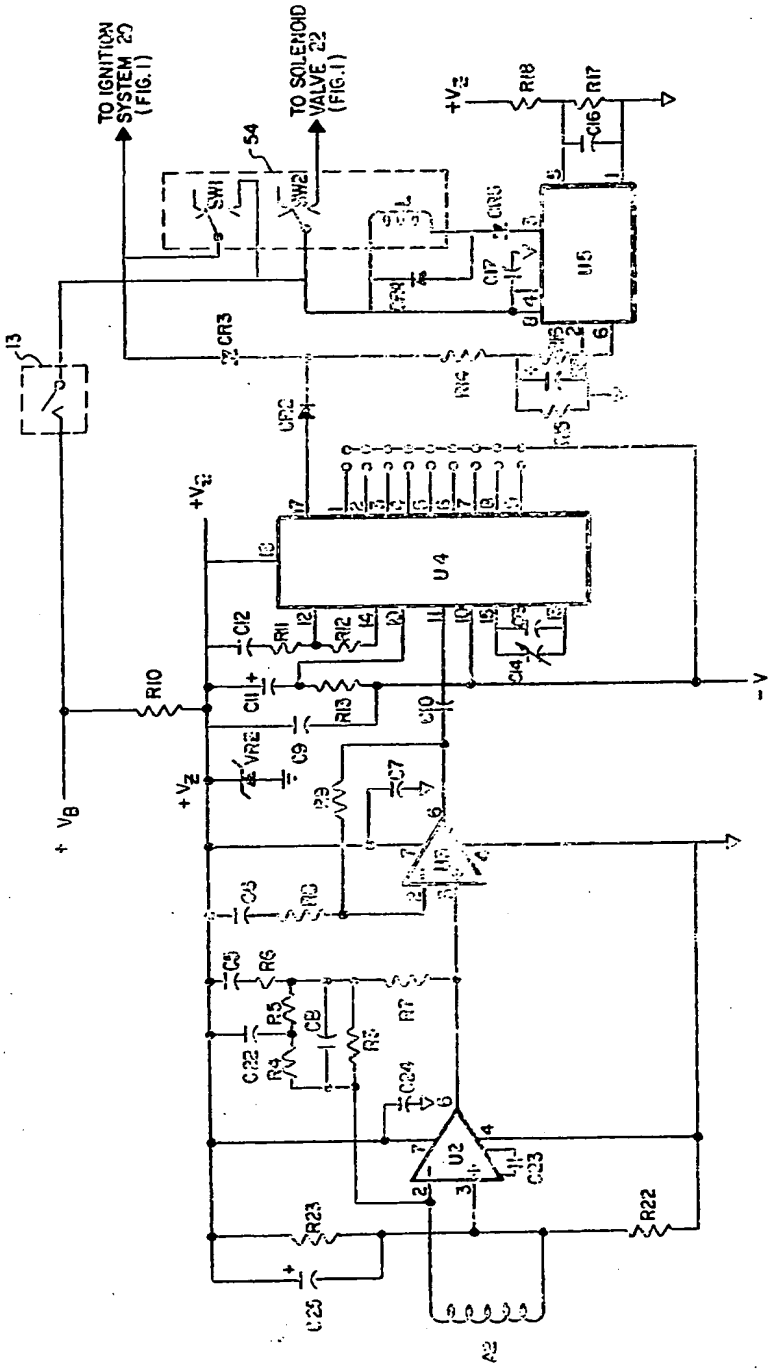

Fig. 4

SPECIFICATION

Security locking system

This invention relates to security locking systems; and more particularly to a security locking system adapted to respond to coded magnetic or electromagnetic signals. The security locking system herein disclosed is particularly useful to prevent the unauthorised use of a vehicle having a spark ignition system; although the locking system could advantageously be used to fill almost any security need.

Security locking systems have been used extensively to prevent the unauthorised entry into a building, safe, or other closed chamber; or to prevent the unauthorised operation of a vehicle or other device. A very common and simple form of security locking system is the use of a lock or switch that is operable only if the user has a key. This is a particularly popular form of security locking system for electrical device that require electrical power in order to operate. That is, it is simple and inexpensive to position a keyed switch between the powered source and the device to be secured. In order to allow operation of the device, the keyed switch must be engaged to allow power to flow from the power source to the device.

The keyed switch approach is used almost universally as a security system for automobiles and other vehicles That is, a keyed switch—referred to as the ignition switch—is connected between the battery and the ignition system of the engine. Before power from the vehicle's battery can energise the ignition system (thereby allowing the engine to run) the ignition switch must be engaged. Engagement of the ignition switch requires a key having the proper configuration. (Other, backup security systems are also known to supplement the keyed switch approach, such as providing locks on the doors of the automobile).

A problem associated with the ubiquitous keyed switch approach, especially as that system is used on automobiles, is the relative case with which the system may be bypassed. In an autombile, for example, an experienced "thief" can easily bypass the ignition switch, or otherwise "hot-wire" thc ignition system, thereby allowing the ignition system to be energized.

Other security locking systems for use with automobiles and the like are generally backup security systems that supplement the ignition switch. These backup security systems typically include warning devices (horns, sirens, and the like) that are triggered if a door, window, or other area of the automobile is entered without deactivating the security system. A timing mechanism is often used in connection with the warning devices so that they are not energized until after a fixed period of time and after entry is made into the vehicle. This time delay allows an authorized user, whose knows how to deactivate the warning devices, to do so after he has entered the vehicle. An unauthorized user, on the other hand, would not know to deactivate the devices and would (hopefully) be frightened off once the warning devices sounded. Unfortunately, these types of systems generally do not prevent operation of the vehicle. Rather, they just make a lot of noise designed to draw attention to the vehicle and its occupant.

Fuel control valves are also known in the art to prevent the unauthorized use of a vehicle. Generally, a means of energizing the fuel valve, thereby allowing fuel to flow from the tank to the engine, is provided through a hidden switch close to the driver's position. An authorized user of the vehicle must energize the valve prior to driving the vehicle. Unfortunately, there is generally enough fuel remaining in the carburetor and fuel line between the control valve and the engine to allow the vehicle to be started and driven a short distance before the effects of the closed fuel control valve are noticed. This can not only be dangerous (as when the vehicle suddenly stops in the middle of the street or other location so as to create a traffic hazzard) but it also can be a source of irritation to an authorized user who forgets to activate the control valve.

Some types of security locking systems utilize an electronic wireless control. The most popular form of such systems are the common electronic garage-door-openers that respond to a signal transmitted from a portable transmitter to a receiver mounted inside of the garage. The receiver responds only to a command signal generated by the transmitter. The receiver is typically carried in an automobile, and must be capable of transmitting a signal over a range of at least 100 feet or so. To properly and accurately transmit a command signal over this range requires that conventional radio frequency broadcasting techniques be utilized within the receiver. That is, a radio frequency (rf) carrier signal must be utilized to carry the command signal from the transmitter to the receiver. The use of such an rf carrier signal increases the cost and complexity of both the transmitting and receiving units. Moreover, it is not uncommon for a given receiver to respond to an improper command signal transmitted by other than the proper transmitter. Because receipt of a command signal is generally the only prerequisite to disarming the security locking system, it thus becomes relatively easy for an unauthorized user to breach the security system.

Magnetically activated security systems are also known in the art. These typically require a magnetically sensitive device to respond to the presence of a magnetic fields. Exemplary systems of this type are disclosed in Avallone,

U.S. Patent No. 3,569,928; Vest, U.S, Patent No. 3,885,164; Peters, U.S. Patent No. 3,962,695; Duke, U.S. Patent No. 4,170,005; and Antenore, U.S. Patent No. 4,136,338. However, all of these systems are responsive to any type of magnetic force field. It is therefore very easy for a counterfeit (or unauthorised) magnetic field to be used to disarm the security devices used in connection therewith.

According to a first aspect, the invention comprises a security locking system for controlling the operation of a device having at least one enabling element that must be energized by a power source for said device to operate, said security locking system comprising distribution means for distributing power from said power source to said enabling element, switch means for controlling power distributed through said distributing means, a receiving unit connected between said switch means and said enabling element for further controlling power distributed through said distribution means in response to the presence of a magnetic field that varies according to a uniquely coded sequence, and a transmitting unit for generating said uniquely coded magnetic field, with said transmitting and receiving units respectively generating and sensing said uniquely coded magnetic field only when said units are in close proximity to each other.

According to a second aspect, the invention comprises an anti-theft prevention method for securing a device having at least one enabling element that must be energized from a power source in order for said device to operate, said prevention method comprising the steps of distributing power from said power source to said enabling element through a power distribution network, connecting a switch in series with said distribution network that switchably controls the delivery of power to said enabling element, connecting a receiving unit between said switch and said enabling element, said receiving unit being adapted to also switchably control the delivery of power to said enabling element in response to sensing the presence of a magnetic field that varies according to a uniquely coded sequence, and placing a transmitting unit in close proximity to said receiving unit and activating the transmitting unit when it is desired to energize said enabling element, said transmitting unit being for generating said uniquely coded varying magnetic field when activated.

The above and other objects, features, and advantages of the invention will be more apparent from the following more particular description presented by way of example in connection with the accompanying drawings, in which:

Figure 1 is a block diagram of the security locking system as it could be used with the components of a conventional automobile;

Figure 2 is a detailed block diagram of the transmitter and receiving units of the locking system;

Figure 3 is an electrical schematic diagram of the transmitter of Fig. 2;

Figure 4 is an electrical schematic diagram of the receiver of Fig. 2; and

Figure 5 is an electrical schematic diagram of a negative voltage supply circuit that can be used to provide the negative voltage needed by the receiver circuit of Fig. 4.

The preferred application of the security locking system herein disclosed is for use with an autombile or similar vehicle. Therefore, the following description of the preferred embodiment primarily relates to use of the security locking system to secure operation of an automobile. However, it is to be understood that a security locking system of the type discussed in this application may be used with any type of device that needs to be secured, and which is controllable through the use of switchable power, or through the use of electromechanical devices that may be controlled by switchable power. Examples of the types of devices that could be secured by a security locking system of this type would include, but are not limited to, doors of dwelling houses and similar buildings, safes, electrical appliances, industrial machinery, and the like.

Referring to Fig. 1, there is shown a basic block diagram of the security locking system as it could be used with the components of a conventional automobile. The security locking system includes a receiving unit 12 and a transmitting unit 14. The conventional components of an automobile that are used in connection with the security locking system include the vehicle's battery 16, the ignition switch 18, and the ignition system 20. A solenoid valve 22 may also be used in connection with the security locking system to control the flow of fuel through a fuel line 24. The fuel line 24 delivers fuel from a fuel tank of the vehicle (not shown) to the engine (also not shown).

In a conventional spark ignition automotive system, power from the battery 16 is delivered to the ignition system 20 through cables or wires 26 and 28. The ignition switch 18 is appropriately placed between the battery 16 and ignition system 20 so as to control, in a secured fashion, the energizing of the ignition system 20. A fuse 30 is also typically used as a safety precaution. This fuse 30 may be placed between the ignition switch 18 and the battery 16. The security locking system modifies the conventional method described above by placing a receiving unit 12 between the ignition switch 18 and the ignition system 20. Thus, the ignition system 20 may only be energized when both the receiving unit 12 is activated and the ignition switch 18 is engaged.

Activation of the receiving unit 12 is illustrated symbolically in Fig. 1 by having the

switch 19 thrown from its "B" position to its "A" position. A magnetically coded signal, represented symbolically as the wavy arrow 32 in Fig. 1, is coupled from the transmitting unit 14 to the receiving unit 12 whenever it is desired to activate the receiving unit. A solenoid valve 22 disposed in the fuel line 24 of the automobile, may also be connected by a wire or cable 34 to the active terminal ("A" of switch 19) of the receiving unit 12. Thus, when the receiving unit 12 is activated by the magnetically coded signal 32, and when the ignition switch 18 is properly engaged, power from the battery 16 may be delivered to both the ignition system 20 and the solenoid valve 22, thereby allowing the vehicle to be operated.

Referring now to Fig. 2, a block diagram of the transmitting unit 14 and the receiving unit 12 are shown. The transmitting unit 14 includes an encoder 40, a driver 42, and a transmitting coil A1. The encoder 40 is energized by a voltage received from a battery B through a push button switch PB. The battery B also serves to energize the driver 42. When the switch PB is engaged, the encoder 40 generates a uniquely coded signal which is presented to the driver 42 over signal line 44. The driver 42, in turn, amplifies the coded signal and presents it to the transmitting coil A1 over signal line 46.

The coded signal generated by the encoder 40 is preferably a digitally coded signal comprising a series of logical ones, zeros, and synchronization bits. A complete coded signal for example, may consist of a data pattern comprised of 16 data bits. Frequency-shift-keying may also illustratively be used to encode the data bit in a suitable fashion. That is, each data bit could be represented by a unique combination of a first and second frequency. For example, if the first frequency is represented by an "H" (for a high frequency) and the second frequency is represented by an "L" (for a low frequency), a logical one might illustratively be encoded as "HH", a logical zero as "HL", and a synchronization bit as "LL". Typically, the frequency of "H" will be double that of "L". As these different frequencies are presented to the transmitting coil A1, the varying currents associated therewith generate a magnetic field around the coil A1 in accordance with well-known principles of magnetic field generation. Thus, a coded magnetic field (represented symbolically as the wavy arrow 32) is present around the coil A1 whenever the push-button switch PB of the transmitting unit 14 is engaged.

The receiving unit 12 includes, as shown in the block diagram of Fig. 2, a receiving coil A2, an amplifier 48, a decoder 40, a timed-latch circuit 52, and a relay 54. The receiving coil A2 is advantageously positioned within the receiving unit 12 so as to be in close proximity to one edge thereof. Thus, when a coded magnetic field 32 is present, this varying magnetic field will induce a voltage in the receiving coil A2 according to well known principles of electromagnetic induction. This induced voltage is presented to the amplifier 48 over signal line 56 where it is amplified and conditioned and presented to the decoder 50 over signal line 58. The decoder 50 compares the received signal to a pre-programmed, or unique, reference signal. If the received signal is the same as the pre-programmed reference signal—that is, if every bit of the received signal matches every bit of a pre-programmed signal—then the decoder 50 generate an output signal on signal line 60. The presence of this output signal on signal line 60 triggers the timed latch 52. This timed latch 52, in turn, is adapted to allow the coil L of the relay 54 to be energized.

The contacts of the relay 54 are connected so as to allow a voltage V_B from the vehicle's battery to be selectively distributed to the ignition system 20 and the solenoid valve 22. Specifically, when the ignition switch 18 is engaged, the voltage V_B from the vehicle's battery 16 is presented over signal line 28 to the relay switches SW1 and SW2. This voltage V_B is also presented to the coil L of the relay 54, although the coil L is grounded only through the timed latch 52 when energized by the output signal of the decoder 50. The relay switches SW1 and SW2 are adapted to remain in their upper, or "off", position as shown in Fig. 2 when the relay coil L is not energized. When the coil L is energized, however, they both are pulled to their lower, or "on", position. Thus, with relay switch SW1 in its "off" position, it is seen that for the configuration shown in Fig. 2, the ignition system 20 is grounded through signal line 29, SW1, and signal line 62. This grounding of the ignition system 20 is, of course, an optional feature which could be easily eliminated by removing the grounding signal line if desired. Further, with SW2 in its off position, it is seen that the solenoid valve 22, which receives power over signal line 34, is not energized. When the relay switches SW1 and SW2 are pulled to their on, or lower, positions, however, it is seen that the battery voltage V_B is routed to the ignition system 20 through switch SW1 and to the solenoid valve 22 through relay switch SW2. Furthermore, this same voltage may be routed through relay switch SW1 to the timed latch circuit 52 over signal line 64. This voltage serves to maintain the timed latch 52 in its on position so as to keep coil L of the relay 54 energized so long as the ignition switch 18 is engaged.

Referring to Fig. 3, there is shown a detailed schematic diagram of the transmitting unit 14. The encoder 40 may advantageously be realized using a commercially available

integrated circuit such as the S274■ Serial Data Encoder manufactured by American Microsystems. Inc. (AMI), and a few discrete passive components. This Serial Data Encoder, labelled U1 in Fig. 3, encodes by means of a frequency-shift-keyed trinary data pattern composed of 16 data bits. Each data bit has a length equivalent to 32 cycles of a high frequency clock. The frequency of this clock is determined by external resistors R1 and R2 and capacitor C1 which are connected as shown. A high frequency clock of 20 kHz is typical. A standard 9–volt battery, represented as B in Fig. 3, may be used to power the Serial Data Encoder U1. The push button switch PB may be connected between the battery B and the encoder U1 so that a single momentary push of the button PB will activate the encoder unit.

The detailed functional and operational characteristics of the Serial Data Encoder integrated circuit U1 are well known in the art and will not be discussed herein. It is sufficient to note that the purpose of the encoder integrated circuit U1 is to provide serial data as an output signal that can be transmitted to a receiving unit. When AMI's S2743 Serial Data Encoder integrated circuit is used to realize U1, this output serial data appears on pin 15. As mentioned above, this data consists of 16 data bits, 9 of which may be selected by the user by selectively grounding or leaving open pins 1 through 9. The remaining 7 bits are fixed for a given unit, and are used to define the beginning and end of a given coded signal, as well as for synchronization purposes.

The driver 42 may be realized using a single transister Q1 (Fig. 3). This transister Q1 may be an NPN transister, such as a generically numbered 2N3904, which has its base connected directly to pin 15 of the integrated circuit encoder U1. The emitter of the transister Q1 is tied to the transmitting coil A1. Current thus flows through the coil A1 as controlled by the encoded signal appearing at the base of transister Q1. A light emitting diode CR1 is connected to the collector of transistor Q1. Hence, all (or almost all) of the current flowing through the coil A1 will also flow through the light-emitting diode CR1. As thus configured, CR1 gives a visual indication that a coded signal is being presented to the transmitting coil A1. The transmitting coil A1, as explained above, generates an alternating magnetic field having frequencies determined by the encoder U1. In the preferred embodiment, these frequencies are between 5 kHz and 10 kHz, although any suitable frequencies could be used.

Alternatively, the driver 42 could be realized by using two transistors connected in a "push-pull" configuration. In such a configuration, one transistor is an NPN and one is a PNP. The emitters and bases of both transistors are connected together, with the common base point being tied directly to the output of the encoder U1, and the common emitter point being tied, typically through a coupling capacitor, to the transmitting coil A1. In such a case, the NPN transistor could illustratively be a 2N3904 and the PNP transistor could be a 2N3906. The primary advantage of such a "push-pull" arrangement, or any other arrangement utilizing a coupling capacitor between the driver and the coil A1, is that it eliminates direct current from flowing in the transmitting coil, which direct current represents a waste of energy.

Referring next to Fig. 4, a detailed electrical schematic diagram of the receiving unit 12 is shown. The alternating magnetic field generated by the transmitting unit 14 induces a signal in the receiving coil A2. This signal is amplified by operational amplifier U2. The output of amplifier U2 is then further amplified by a voltage follower consisting of another operational amplifier U3. The operational amplifier U2 may be realized using a commercially available integrated circuit, such as the CA3130, while the voltage follower operational amplifier U3 may be realized using the commercially available operational amplifier CA3140, both of which are manufactured by RCA.

The output of the voltage follower U3 is presented through a coupling capacitor C10 to a Serial Data Decoder integrated circuit U4. This Serial Data Decoder U4 is equivalent to the decoder 50 shown in Fig. 2. A commercially available Serial Data Decoder, such as the S2742 manufactured by AMI, may be used to realize the decoder U4 in the preferred embodiment. Such a decoder decodes the transmitted 16 bit coded signal using on-chip phase-locked-looped techniques. Conventional comparison techniques are also employed to compare the decoded signal with an externally selected code. The pins of U4 numbered 1 through 9 in Fig. 4 may be programmed by a user to correspond to the code set by the user in connection with the encoder integrated circuit U1 of Fig. 3. Thus, a user may set nine of the bits of the sixteen bit coded word in any desired sequence known only to the user, thereby maintaining the integrity and secrecy of the device.

The functional and operational description of the decoder integrated circuit U4 is well known in the art, and will not be presented herein. It is sufficient to note that when a coded signal is received by the integrated circuit U4 that matches the pre-programmed reference determined by selective definition of the nine selectable bits, an output signal appears on pin 17 of the device. This output for the S2742 Serial Data Decoder manufactured by AMI, is a high voltage level. When present, this high voltage level allows current to flow from the decoder U4, through both the

diode CR2 and resistor R14, to the capacitor C15. The voltage at the positive side of this capacitor thus rises with a time constant primarily set by the value of capacitor C15 and the value of resistor R14. As this voltage rises to a certain threshold, the timing circuit U5 is triggered. The valve of this switching threshold is set by the voltage divider network formed by resistors R17 and R18. Capacitor C16 is used as a bypass capacitor to filter noise from this threshold level.

The timing circuit U5 may be realized using a generically numbered commercially available 555 timing circuit, now manufactured by numerous semi-conductor manufacturers such as Signetics, Fairchild, National, and RCA. So long as the voltage at pins 2 and 6 of U5 exceeds the specified threshold, current may flow into pin 3 to ground, thereby energizing coil L of relay 54. However, should the voltage at pins 2 and 6 drop below the triggering threshold level, the coil L of relay 54 will be de-energized.

An additional diode CR3 is connected between the wiper of relay switch SW1 and the cathode of diode CR2. This diode CR3 allows the battery voltage V_B to be applied to the capacitor C15 once the relay 54 is initially energized. A high voltage at pin 17 of the decoder U4, even if only momentary (i.e., a pulse), is initially required to energize the relay 54. As explained above, this high voltage charges capacitor C15 above a threshold level so as to trigger the timing circuit U5. Once triggered, U5 responds by grounding the coil L of the relay 54 through diode CR5. During this time, current is allowed to flow through the coil L, thereby energizing the relay coil and throwing the relay switches SW1 and SW2 to their "on", or lower, positions. With relay switch SW1 in its "on" position, it is seen that battery voltage V_B is presented through diode CR3 back to the capacitor C15. Thus, C15 remains charged above the threshold level, thereby maintaining the relay 54 in its energized condition. In this fashion, the relay 54 remains latched on until such time as the ignition switch 18 is used to interrupt the battery voltage V_B.

It would also be possible to configure the timed latch 52 (Fig. 2) such that should the voltage on line 60 drop below a threshold triggering level of the timed latch 52, the relay 54 would nonetheless remain energized for a prescribed time period. This time period could be selected to be sufficiently long so as to enable a user of the security locking system to (1) transmit a coded magnetic signal from the transmitting unit 14 to the receiving unit 12, and (2) to engage the ignition switch 18 with an ignition key. With such a configuration, the sequence of activating the receiving unit 12 and engaging the ignition switch 18 could thus be reversed.

Should the ignition switch 18 be disengaged, the capacitor C15 (Fig. 4) will hold a voltage above the threshold triggering level for a period of time set primarily by the value of resistor R15 and the value of capacitor C15. Thus, a user may momentarily disengage the key switch 18 without having to retransmit another magnetically coded signal from the transmitting unit 14.

As is apparent from Fig. 4, a zener diode, VRZ, may be used to regulate the battery voltage V_B to a more precise value. Where the battery voltage V_B is 12 volts, which is common for most automobiles, the zener diode VRZ may illustratively by a 1N4740, or a 10 volt zener diode. This regulated zener voltage is then used to power the integrated circuits U2, U3, U4, and U5. The use of the zener diode VRZ is optional inasmuch as all of the integrated circuits will operate from an unregulated voltage source. However, the use of the zener diode VRZ does provide some measure of overvoltage protection to these devices. It also serves to more precisely define the threshold switching and time constants associated with the operation of the timing circuit U5.

The decoder circuit U4 requires a negative voltage, $-V$, as well as a positive voltage, in order to operate. Such a negative voltage is typically not available within the electrical system of a standard automobile. Accordingly, a negative voltage supply, such as that shown in the schematic diagram of Fig. 5, may be used to generate the requisite negative voltage from the positive zener voltage, V_z. The circuits shown in Fig. 5 include an oscillator having a frequency of around 100 kHz. This oscillator is realized using inverting logic gates 70 and 72 connected in series in a common oscillator circuit configuration. Capacitor C19 is alternatively charged and discharged through resistor R20 as the states of the logic gates 70 and 72 changes. Resistor R19 prevents C19 from discharging into the input protection circuits of gate 70, thereby stabilizing the frequency of oscillation. Logic gates 74, 76, 78, and 80 are connected in parallel and comprise a buffer amplifier that conditions and buffers and oscillator output. Once buffered, the amplifier output is presented to a one-half wave voltage doubler consisting of capacitors C20 and C21, diodes CR6 and CR7, and resistor R21. A typical value for the negative voltage thus generated, assuming a positive input voltage of + 10 volts, is on the order of negative 7 or 8 volts. The inverting logic gates may advantageously be realized in a single CMOS hex inverting integrated, circuit, such as the CD4049 manufactured by numerous semiconductor manufacturers.

The circuits shown in Figs. 3, 4 and 5 may be readily realized by those skilled in the art using commercially available components based on the above description. The majority of the capacitors and resistors shown in these

figures are for bias and stabilization purposes, and those skilled in the art will readily recognize the values and particular network that must be used with such components in order to allow the various integrated circuits and other active devices to operate. The transmitting coil A1 (Figs. 2 and 3) may be realized by winding about 350 turns of No. 40 wire over a ferrite core, such as commercially available core No. R33–050–400, available from Amidom. Similarly, the receiving coil A2 (Figs. 2 and 3) may also be realized using an Amidom ferrite core, R33–050–750 over which approximately 350 turns of No. 40 wire have been wound.

The simplicity of the transmitting unit 14 allows it to be realized in a relatively small, hand-held, unit. Thus realized, the unit may be conveniently placed in a shirt pocket or purse where it would be as readily available to an authorized user as is a conventional key. The battery B, used in connection with the transmitting unit 14, may also be a small, inexpensive, commercially available battery, such as a 9 volt Model 246 manufactured by Burgess, or the Model 216 manufactured by Eveready.

The receiving unit 12 may also be realized in a relatively compact area, and thus can be mounted within an automobile or dwelling unit in a hidden location that is close to the point of entry or location of operation. For example, when used with an automobile, the receiver may be mounted under the dash close to the driver's seat. Once mounted. It is a relatively simple matter to connect it to the ignition switch 18, the ignition system 20, and the solenoid valve 22, as well as ground, as shown in Fig. 1. A typical set of instructions for mounting the receiving unit 12 within an automobile are as follows:

1. Mount the receiving unit 12 inside of the vehicle near the driver's position, preferably in a location where it is not visible.

2. Locate the wire going from the ignition switch 18 to the ignition system 20. (This is signal line 28 in Fig. 1.) This signal line 28 is the wire going to the coil of a conventional ignition system or to the control module of an electronic ignition system. This signal line typically has a voltage of between + 11 to + 14 volts when the ignition switch is engaged and zero volts when the ignition switch is disengaged. No connections should be made to the secondary (high voltage) part of the ignition system. No other connection should be made to any of the wires associated with the ignition system, including the wire from the coil to the distributor.

3. Break the wire located in step 2 (signal line 28 in Fig. 1.)

4. Determine which end of the wire broken in step 3 connects to the battery through the ignition switch 18. This will be the end that has 12 volts on it when the ignition switch is engaged. Connect wire 27 from the receiving unit 12 to this battery end of the wire 28.

5. Connect the wire 29, also coming from the receiving unit 12, to the other end of the wire broken in step 3. This is the end of wire 28 that connects to the ignition system 20.

6. Connect the wire 52 coming from the receiving unit to a good ground, such as the frame of the vehicle.

7. Connect the wire 34 coming from the receiving unit 12 to one of the wires of the solenoid valve 22.

8. Connect the other wire on the solenoid valve 22 to a good ground, such as the frame of the vehicle.

When the system is carefully connected according to the above set of instructions, the transmitting unit 14 may be used to arm the receiving unit 12 with a properly coded signal. Once properly armed, the receiving unit 12 allows the vehicle—including its ignition and fuel system—to be operated in a conventional manner. However, if the receiving unit 12 is not armed properly, then the vehicle will not start. Moreover, even if it somehow could be started, it would not operate very long inasmuch as the fuel system would be inhibited.

It is significant to note that the coded signal coupled between the transmitting and receiving units is merely a specified sequence of a changing magnetic field. That is, no rf carrier signal is employed to carry the coded signal from the transmitting unit to the receiving unit.

While the invention herein disclosed has been described by means of specific embodiments and applications thereof, numerous modifications and variations could be made thereto by those skilled in the art without departing from the scope of the present invention as defined by the claims. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

CLAIMS

1. A security locking system for controlling the operation of a device having at least one enabling element that must be energized by a power source for said device to operate, said security locking system comprising distribution means for distributing power from said power source to said enabling element, switch means for controlling power distributed through said distribution means, a receiving unit connected between said switch means and said enabling element for further controlling power distributed through said distribution means in response to the presence of a magnetic field that varies according to a uniquely coded sequence, and a transmitting unit for generating said uniquely coded magnetic field, with said transmitting and receiv-

ing unit respectively generating and sensing said uniquely coded magnetic field only when said units are in close proximity to each other.

2. A security locking system according to claim 1 wherein said coded magnetic field comprises an oscillating magnetic field that oscillates at first and second frequencies, said first and second frequencies sequentially appearing within said coded magnetic field according to a unique repetitive pattern.

3. A security locking system according to claim 2 wherein said unique repetitive pattern comprises a trinary logical sequence including a unique series of logical 1's, 0's, and synchronization bits, said logical 1's, 0's, and synchronization bits each being defined by a unique combination of said first and second frequencies.

4. A security locking system according to claim 3 wherein said first frequency is at least double said second frequency.

5. A security locking system as claimed in any one of claims 1 to 4 wherein said device to be controlled is a vehicle, said power source is the vehicle's battery, said enabling element is the vehicle's ignition system, and said switch means is an ignition switch having on and off positions.

6. A security locking system according to claim 5 and further including an additional enabling element comprising valve means disposed in a fuel line of said vehicle for controlling the flow of fuel through said line, said valve means being controlled by said receiving unit in response to sensing the presence of said uniquely coded magnetic field.

7. A security locking system according to any one of claims 1 to 6 wherein said receiving unit includes sensing means for sensing the presence of a varying magnetic field and generating a varying signal in response thereto, said varying signal having variations therein that follow the variation of said sensed magnetic field, amplifying means for amplifying and conditioning said varying signal, decoder means for determining whether the variations in said amplified and conditioned varying signal occur in a pattern and sequence corresponding to a pre-programmed code, and for generating an enabling signal when said pre-programmed code is determined to be present in the variations of said varying signal, and relay switch means responsive to said enabling signal for allowing said at least one enabling element to be energized by said power source through said distribution means when said relay switch means is in a first position, and for not allowing said at least one enabling element to be energized when said relay switch means is in a second position.

8. A security locking system according to claim 7 wherein said relay switch means further includes grounding means for electrically grounding said at least one enabling element when said relay switch means is in said second position.

9. A security locking system according to claim 7 or claim 8 wherein said receiving unit further includes a timing circuit adapted to place said relay switch means in said first position for a prescribed period of time after said enabling signal has been generated.

10. A security locking system according to claim 9 wherein said receiving unit further comprises latching means responsive to said enabling signal for latching said relay switch means in said first position for so long as said switch means is turned to its on position.

11. A security locking system according to claim 9 or claim 10 wherein said timing circuit further includes holding means for holding said relay switch means in said first position for a period of time after said switch means has been turned to its off position.

12. A security locking system according to any one of claims 1 to 11 wherein said transmitting unit comprises encoder means for generating a uniquely coded signal that varies according to a selectively coded sequence, driver means for amplifying and conditioning said uniquely coded signal, magnetic generation means for generating a varying magnetic field that varies according to said uniquely coded signal, a second battery, and a transmitting switch electrically connected between said second battery and said encoder, driver, and magnetic generation means for allowing said means to be energized by said second battery when said transmitting switch is placed in a transmit position, and for not allowing said means to be energized when said transmitting switch is placed in a non-transmit position.

13. A security locking system according to claim 12 wherein said transmitting unit further includes an indicator that visually signals when said transmitting unit is generating said uniquely coded magnetic field.

14. An anti-theft prevention method for securing a device having at least one enabling element that must be energized from a power source in order for said device to operate, said prevention method comprising the steps of distributing power from said power source to said enabling element through a power distribution network, connecting a switch in series with said distribution network that switchably controls the delivery of power to said enabling element, connecting a receiving unit between said switch and said enabling element, said receiving unit being adapted to also switchably control the delivery of power to said enabling element in resonse to sensing the presence of a magnetic field that varies according to a uniquely coded sequence, and placing a transmitting unit in close proximity to said receiving unit and activating the transmitting unit when it is desired to energize said enabling element, said transmitting unit being for generating said uniquely coded varying

magnetic field when activated.

15. A security locking system substantially as hereinbefore described with reference to the accompanying drawings.

16. An anti-theft prevention method substantially as hereinbefore described with reference to the accompanying drawings.

Printed for Her Majesty's Stationery Office
by Burgess & Son (Abingdon) Ltd.—1982.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained